FDIC

FEDERAL DEPOSIT INSURANCE CORPORATION

Information Technology

Information Technology – Session Structure

- Board of director actions
- Significant and emerging IT risks
- Practical questions
- Resources

Compensating Controls at the Directorate Level

- **IT governance**
  - Board of Directors
  - Committee of the Board of Directors
    - IT Committee
    - IT Steering Committee
    - Audit Committee
- **Strategic plan**
  - Consistent direction
  - Management skills

Compensating Controls at the Directorate Level (cont.)

- **Risk assessment**
  - Assess applicable threats, their likelihood and impacts, and mitigating controls
  - Identify any additional mitigating actions that may be necessary
    - Support for IT initiative

Compensating Controls at the Directorate Level (cont.)

- **Policies**
  - Information security programs
  - Identity theft prevention programs
  - Incident response plans
  - Business continuity
  - Vendor management programs
  - Acquisition and programming standards
  - Configuration management standards and patch management programs
  - Wire transfer and Automated Clearing House policies

Compensating Controls at the Directorate Level (cont.)

- **IT Audit Programs**
  - IT-related policies and standards (i.e., business continuity, information security, vendor management, wire transfer and automated clearing house activities)
  - IT general control reviews
  - Internal and external vulnerability assessments
  - Penetration tests
- **Audit and regulatory exception tracking tools**
  - Exceptions receive proper attention

Compensating Controls at the Directorate Level (cont.)

- **Board Reports**
  - Information security programs and identity theft prevention programs (required at least annually)
  - Initial and ongoing service provider reviews
    - Service provider relationships: financial statement reviews, audit findings, business continuity test results, and regulatory examination report findings

Significant and Emerging IT-Related Risk Considerations

- Third-party payment processor relationships (payment processors)
- Corporate account takeovers (account takeovers)
- Distributed denial of service attacks
- Outsourcing

Payment Processors

- Due diligence, close monitoring, and prudent underwriting
- Risk assessment
- Policies and procedures (including agreements and contracts) for due diligence, underwriting, and monitoring
- Consumer complaints or unusual automated clearing house return rates
- Response programs

Payment Processors – Board Considerations

- **Strategic**
  - Is the relationship consistent with the bank’s strategic objectives?
  - Are payment processors, its clients, and their industries representative of the bank’s market and areas of expertise?
  - How will the Board ensure that the processor will comply with credit risk, account security, service availability, audit, and reporting policies?

Payment Processors – Board Considerations

- **Risk Assessment**
  - Has the Board ensured management has considered the risks within the risk assessment?
  - How will those risks, such as merchant data breaches, fraud, and credit and reputational risk, be mitigated?
- **Policy and Procedure**
  - Have policies and procedures been revised to account for the responsibilities and mitigating controls applicable for payment processor relationships?
  - Has the Board ensured adequate legal review over agreements and contracts?

Payment Processors – Board Considerations (cont.)

- **Audit**
  - Does the bank retain the right to audit payment processors?
  - Does the scope of the audit programs address payment processor risks?
- **Reporting**
  - What reports will the Board receive to monitor payment processor activities and conformance with approved risk tolerances?

Account Takeovers – Board Considerations

- **Strategic**
  - Are there adequate management capabilities to mitigate this risk or does the bank need to outsource?
- **Risk Assessment**
  - How has the information security risk assessment been updated to reflect emerging risks from account takeover activities?
  - What additional control structures have been implemented to mitigate these risks?
- **Policy and Procedure**
  - How have the bank's policies and procedures been revised to prevent, detect, and respond to account takeovers?

Account Takeovers – Board Considerations (cont.)

- **Audit**
  - How do the bank’s Internet banking, wire transfer, and Automated Clearing House audits assess the bank’s programs for preventing, detecting, and responding to account takeover activity?
  - Is the frequency of such audits consistent with the inherently high-risk nature of electronic funds transfer activity?
- **Reporting**
  - What mechanisms are in place to keep the Board apprised of account takeover activity?

Distributed Denial of Service Attacks

- Designed to disrupt banking services
- Could slow or interrupt a bank's access to external on-line applications
- Typically do not affect safety of customer accounts

Distributed Denial of Service Attacks – Board Considerations

- **Risk Assessment**
  - Has the information security risk assessment been updated to reflect the changing threat scenario of such attacks?
  - What additional actions have the Board facilitated to mitigate these threats?
- **Policy and Procedure**
  - Have the bank's policies and procedures (particularly incident response plans) been revised to respond to distributed denial of service attacks?
- **Audit**
  - Do business continuity or incident response audits assess the bank's readiness for distributed denial of service attacks?
- **Reporting**
  - What mechanisms are in place to keep the Board apprised of these events?

Outsourcing

- Banks retain partial or full ownership of several key risks

- Types of risks may include:
  - Operational
  - Transactional
  - Strategic
  - Legal
  - Regulatory
  - Reputational
  - Financial

Outsourcing – Board Considerations

- **Strategic**
  - Are outsourcing arrangements consistent with the bank's strategic objectives?
  - Are agreements in place to ensure service providers share sufficient information to oversee such relationships and meet strategic objectives for information security?
- **Risk Assessment**
  - Are all significant vendor and outsourcing relationships (by platform and location) accounted for in the information security risk assessment?
  - What residual risks will the bank retain?
  - What can be done to further reduce this level of risk?

Outsourcing – Board Considerations (cont.)

- **Policy and Procedure**
  - Do vendor management programs extend to all significant service providers, platforms and locations?
- **Audit**
  - Do service providers provide routine audits of the platforms and locations that support the bank’s outsourcing arrangements?
  - Has the Board received and reviewed IT reports of examination for the platforms and locations of its service providers?

Outsourcing – Board Considerations (cont.)

- **Reporting**
  - What reports will the Board receive to ensure that bank management has executed proper oversight of vendors and service providers?
  - How frequently will they be provided?

Summary

- Board and committee oversight
- Strategic plans
- Risk assessments
- Policies and procedures
- Audits
- Reports

Resources

- **Payment Processors**
  - Revised Guidance on Payment Processor Relationships (FIL-3-2012)
  - "Managing Risks in Third-Party Payment Processor Relationships," Summer 2011 Supervisory Insights Journal article
- **Account Takeovers**
  - FFIEC Supplement to Authentication in an Internet Banking Environment (FIL-50-2011)
  - FFIEC Guidance: Authentication in an Internet Banking Environment (FIL-103-2005)
- **Distributed Denial of Service Attacks**
  - Understanding Distributed Denial of Service Attacks:

Resources (cont.)

- **Technical assistance from federal agencies specializing in cyber security**
- **Outsourcing**
  - Foreign-Based Third-Party Service Providers Guidance on Managing Risks in These Outsourcing Relationships (FIL-52-2006)
  - New Guidance for Examiners, Financial Institutions and Technology Service Providers on Management and Outsourcing Technology Services (FIL-89-2004)
  - Bank Technology Bulletin on Outsourcing (FIL-50-2001)
  - FFIEC IT Examination Handbook
  - Outsourcing Technology Services Booklet

Resources (cont.)

- Additional Videos
- Directors' Resource Center: http://www.fdic.gov/regulations/resources/index.html
- Mailbox: supervision@fdic.gov